




INTERNAL MANAGEMENT POLICY & PROCEDURE	SECTION NUMBER 05-105	PAGE NUMBER 1 of 11
	CHAPTER & SUBJECT: INFORMATION TECHNOLOGY AND RECORDS: KCJIS Web Browser Tokens	
Approved By:  Commissioner of the Juvenile Justice Authority		Original Date Issued: 10/27/00 Current Amendment Effective: 11/29/06 Replaces Amendment Issued: 10/27/00

POLICY

The Juvenile Justice Authority shall establish procedures to provide staff and the TAC Officer with directions for the assignment of tokens and security procedures for those tokens when accessing information through the Kansas Criminal Justice Information System (KCJIS).

DEFINITIONS

Tele-communications Access Coordinator (TAC): A designated employee within the Information Technology and Research Division who ensures the security procedures are maintained through the assignment of tokens to access KCJIS.

Token: An individually assigned electronic device used to display access codes. Access codes change on this device every 60 seconds.

PROCEDURE

I. Introduction

- A. The agency uses a web access terminal to obtain information through the KCJIS system. To make the system more secure there is a system where operators are issued tokens to provide access codes. The tokens shall only be issued to terminal operators and the agency TAC Officer.

II. Issuance of Tokens

- A. The agency TAC Officer shall control and issue tokens for KCJIS. The TAC Officer shall maintain records concerning the tokens. Prior to issuance, the staff member shall complete the limited access terminal operator training, and the KCJIS class.
- B. Staff receiving a token shall maintain the security and safety of the token assigned.
- C. Tokens shall not be loaned to other staff members. Each staff member shall be responsible for any records obtained under their token identification.
- D. When the TAC Officer is issuing a token, he/she shall complete all the forms in the Token Packet, Attachment A. The TAC and terminal operator shall complete the token checklist to insure all steps and procedures, as required by KCJIS and NCIC, are followed.

III. Resignation and Termination of Employees

- A. Upon the resignation or termination of a terminal operator, that operator's token shall be turned in and access to the terminal ceased. If an employee is terminated, that employee shall immediately return the token to the TAC Officer. The TAC Officer shall immediately contact the KBI communications section and advise them the employee was terminated and the token was returned.
- B. In cases where the employee takes a voluntary termination, he/she shall return the token to the TAC Officer on the last day of employment. The TAC Officer shall secure the token and contact the KBI to advise them the employee has voluntarily terminated employment and the token shall be deactivated. All KCJIS tokens returned shall be secured by the agency TAC Officer.

IV. Spare Tokens/Non Functioning Tokens

- A. Any spare tokens shall be deactivated, secured, and not used until they are reassigned.
- B. Juvenile Justice Authority shall not have activated spare tokens for use. Staff members shall only use tokens individually assigned to them. If a token is not operating correctly, it shall be returned to the agency TAC Officer.
- C. The agency TAC Officer shall notify the KBI Communications Section that the token is not functioning and to deactivate the token. He/she shall then reactivate any "spare" tokens or request a new token.

V. Lost or Stolen Tokens

- A. If a token is lost or stolen it shall be immediately reported to the agency TAC officer. A lost or stolen report shall be filed with the law enforcement agency of jurisdiction. The case number shall to be supplied to the agency TAC Officer.
- B. When the agency TAC Officer is notified of the loss or theft, he/she shall immediately notify the State KCJIS Security Officer and the Kansas Bureau of Investigation Communications Section of the loss or theft.
- C. If the employee is advised of the recovery of a lost or stolen token, he/she shall contact the agency TAC Officer to recover the token. The agency TAC Officer shall notify the KCJIS Security Officer that the token has been recovered.

VI. Violation of This Policy

- A. Violation of this policy shall result in disciplinary action up to and including immediate removal from terminal access and dismissal.

NOTE: The policy and procedures set forth herein are intended to establish directives and guidelines for staff and juveniles and those entities that are contractually bound to adhere to them. They are not intended to establish State created liberty interests for employees or juveniles, or an independent duty owed by the Juvenile Justice Authority to employees, juveniles, or third parties. This policy and procedure is not intended to establish or create new constitutional rights or to enlarge or expand upon existing constitutional rights or duties.

REPORTS REQUIRED

None.

REFERENCES

None.

ATTACHMENTS

Attachment A: Token Packet, 9 Pages.

TOKEN PACKET

SecurID Key Fob

You have been assigned a standard SecurID® Key Fob to use when logging in. These security tokens generate and display unpredictable codes that change at a specified time (every 60 seconds).

To gain access to the protected system, you must enter a valid SecurID PASSCODE™ that is made up of two factors:

- ☐ your secret, memorized personal identification number (PIN)
- ☐ the tokencode currently displayed in your SecurID Card or Key Fob

With a conventional security system it is easy for someone to learn your password and log in under your identity. Requiring two factors ensures reliable identification and authentication.

Because this system creates an audit trail that cannot be repudiated, you may be held accountable for activities recorded identifying you as the perpetrator. Avoid the unauthorized use of your identity and privileges by protecting the secrecy of your PIN and the possession of your token. Read "User Responsibilities" on page 5 to learn about your obligations as a token holder.

Before You Begin

If you have any questions, contact KBI Communications, at extension 785-296-8262.

- ☐ You will be allowed to use a PIN that you make up yourself.
(Read "Creating Your Own PIN") OR
- ☐ You can allow the system to generate your PIN for you.
(Read "Creating Your Own PIN" on page 2.)
- ☐ Your PIN may contain only numbers.
- ☐ All PINs on the system can be 4 - 8 digits.
- ☐ All tokens are sent in New PIN mode.

*Kansas Criminal Justice Information System
SecurID Key Fob*

Receiving A System-Generated PIN

1. Open your Internet browser i.e. Internet Explorer, Netscape. Go to the KCJIS web page at <http://www.kcjis.state.ks.us>. A KCJIS SecurID Passcode web page will appear.
2. Type in your KCJIS user ID.
3. Your token is in New PIN Mode, in the **PASSCODE** box, type the tokencode that is currently displaying in your SecurID token. **NO PIN** number.

(If your token previously had a PIN and the administrator did not clear it when setting it into New PIN mode, enter the old PIN followed by the tokencode that is currently displaying in your SecurID token.)

4. Click **Send**.

If the system displays **User access denied**, click **OK** and try again.

5. Once you enter a valid code, the New PIN web page will be displayed.
6. The web page asks if you are ready to setup your new PIN. Make sure that no one can see your screen.
7. Click the radio button beside System-generated PIN.
8. Click on the Send button.

A system-generated PIN displays for 10 seconds. Memorize the PIN; **DO NOT WRITE IT DOWN**.

9. Click on Continue.
10. A web page appears asking you to test your new pin. Type in your KCJIS User ID. In the **PASSCODE** box, type your PIN followed by the tokencode currently displaying in your card or key fob.
11. A SecurID Passcode web page will appear requesting your KCJIS user ID and Passcode again. Wait for the next tokencode, and then follow the instructions in "SecurID Authentication" on page 4.

Creating Your Own PIN

1. Before you create your own PIN, give some thought to what it will be. Do not pick an obvious number like a birthday or phone number.
2. Open your Internet browser (i.e. Internet Explorer, Netscape). Go to the KCJIS web page at <http://www.cjis.state.ks.us>. A KCJIS SecureID Passcode web page will appear.
3. Type in your KCJIS user ID.
4. Your token is in New PIN Mode, in the **PASSCODE box**, type the tokencode that is currently displaying in your SecurID token.

(If your token previously had a PIN and the administrator did not clear it when setting it into New PIN mode, enter **the** old PIN followed by the tokencode that is currently displaying in your SecureID token.)

5. Click **Send**.

If the system displays User access denied, click OK and try again.

6. Once you enter a valid code, the New PIN web page will be displayed.
7. The web page asks if you are ready to setup your new PIN. Make sure that no one can see your keyboard.
8. Click on the radio button beside "I will create my PIN."
9. Enter your PIN, and press TAB. Enter your PIN again to confirm.
10. Click on the Send button.

If any of the following messages display, try again:

PIN and confirmation do not match.

PIN must be 4-8 digits.

New PIN rejected.

11. After successfully setting up your PIN, a web page appears asking you to test your new pin. Type in your KCJIS User ID in the User Name box. In the PASSCODE box, type your PIN followed by the tokencode currently displaying in your card or key fob.
12. Click on the Send button.
13. A SecurID Passcode web page will appear requesting your KCJIS user ID and Passcode again. Wait for the next tokencode, and then follow the instructions in "SecurID Authentication" on page

The "Next Token Code" Prompt

On occasion, even after you type your PASSCODE correctly, the system prompts you to enter the next tokencode that appears in order to confirm your possession of the SecurID token.

Wait until the tokencode changes, carefully type the new one, and click **OK**.

If you are not granted access after correctly entering the next tokencode, contact your security administrator.

User Responsibilities

You are responsible for protecting the authentication factors entrusted to you. Keep your PIN secret and protect your SecurID token against loss and theft.

If an unauthorized person learns your PIN and obtains your token, this person can assume your identity. Any action this intruder takes is attributed to you in the system's security log.

For your own protection and that of the system always take the following precautions:

- Never reveal your PIN or user password to anyone. Do not write them down.
- If you think someone has learned your PIN, notify the security administrator, who will clear the PIN immediately. At your next login you will have to receive or create a new PIN.
- Exercise care not to lose your SecurID token or to allow it to be stolen. If your token is missing, tell an administrator immediately. The administrator will disable the token so that it is useless to unauthorized users, or assign you a temporary password.
- Do not let anyone access the system under your identity (that is, log in with your PIN and a tokencode from your SecurID token).
- It is essential to site security that you follow your system's standard logoff procedures. Failure to log off properly can create a route into the system that is completely unprotected.
- Protect your token from physical abuse. Do not immerse it in liquids, do not expose it to extreme temperatures, and do not put it under pressure or bend it. Read and follow the care instructions that come with your SecurID token.

Employees/Administrators who receive token.

Token Receipt Form

I, _____, as an employee of

_____ Juvenile Justice Authority of Kansas _____ acknowledge that that I have received my SecureID token with serial number _____ (on back of token). Along with my token I have received instructions on care of the token and information regarding the security of the token. With this I understand that if my token is lost/stolen I need to report this to my supervisor immediately and that the responsibility to replace this token is up to my agency or me not KCJIS. If I fail to report the loss of my token I understand that I am liable for any use of the token while it is not under my control. I also understand that under no circumstances am I to share my PIN number with anyone else or let anyone else use my token to access the system.

Signature

Date

This must be faxed to 785-296-6781 before token is enabled.

TOKEN INSTRUCTION CHECK LIST

AS THE TAC REVIEWS EACH OF THE ISSUES BELOW, THE TAC AND THE OPERATOR TO BE ASSIGNED THE TOKEN SHALL INITIAL THE FORM. THE OPERATOR SHALL THEN COMPLETE THE FORM ON THE NEXT PAGE.

INITIALS**OPERATOR TAC**

_____	_____	Completed less than full access training
_____	_____	Completed terminal training from Trainer
_____	_____	Function of token
_____	_____	Importance of security token
_____	_____	Token not to be shared
_____	_____	Procedure if token lost or stolen
_____	_____	Importance of appropriately logging off the system

SecureID Token Deployment

As an employee of Juvenile Justice Authority, my job duties require that I have access to the Kansas Criminal Justice Information System. (KCJIS) In order to gain access to the information needed for my job duties I will be assigned a SecureID token.

I understand that I am responsible for the security of this token, and that I will not share my PIN number (the number that only you know) with any other person. When I am not operating the system I understand that it is important that I sign off the system or lock my computer so that no other person can use my computer and my identity.

If my token is lost/stolen I must report this to my TAC and supervisor immediately, who will then report this to KBI communications at 785-296-8262 immediately. If I fail to report the loss of my token, I understand that I am liable for any use of the token while it is not under my control. I also understand that failure to report the loss of my token could be considered grounds for disciplinary action. I will also be responsible for the replacement cost of the token.

I have been provided with the following and by signing below I acknowledge that I have received:

1. A copy of the instructions for care of SecureID tokens
2. A copy of the State of Kansas Security Policies
3. Instructions on locking my computer
4. My secure ID token

Signature

Date

SecurID Authentication

Follow the procedure in this section whenever you need to be authenticated to the KCJIS system:

1. In the User Name dialog box, type your KCJIS user name.
2. At the **Enter PASSCODE** prompt, type your PIN followed by the tokencode currently displaying in your card or key fob.
3. Click **OK** or **Send**

If the system displays **User access denied**, you may have typed your PASSCODE incorrectly. Try again.

Once accepted, SecurID PASSCODEs cannot be used again. To log in again, you must wait for a new tokencode to appear. The new tokencode appears after the last of the countdown indicators disappears from the left of the LCD.

If you are repeatedly denied access even though you are typing your PASSCODE correctly, contact KBI Communications at 785-296-8262.